

<b>Notice of Allowability</b>	<b>Application No.</b>	<b>Applicant(s)</b>	
	09/818,914	HOPKINS ET AL.	
	<b>Examiner</b>	<b>Art Unit</b>	
	Paul Callahan	2137	

**-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--**

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to Amendment filed 4/17/06.
2. ☒ The allowed claim(s) is/are 1-5, 7-9, 11-16, 18, 20-24, 26, 28, 29, 31-36, 38-46, 48-52, 54, 56, 60 and 62-66.
3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
  - a) ☐ All    b) ☐ Some\*    c) ☐ None    of the:
  1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

\* Certified copies not received: \_\_\_\_\_.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.  
**THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.**

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
  5. ☐ CORRECTED DRAWINGS ( as "replacement sheets") must be submitted.
    - (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review ( PTO-948) attached
      - 1) ☐ hereto or 2) ☐ to Paper No./Mail Date \_\_\_\_\_.
    - (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date \_\_\_\_\_.
- Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).**
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

**Attachment(s)**

- |   |  |
|---|--|
| 1. <input type="checkbox"/> Notice of References Cited (PTO-892)  | 5. <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)            |
| 2. <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)                                | 6. <input type="checkbox"/> Interview Summary (PTO-413),<br>Paper No./Mail Date _____. |
| 3. <input type="checkbox"/> Information Disclosure Statements (PTO-1449 or PTO/SB/08),<br>Paper No./Mail Date _____ | 7. <input checked="" type="checkbox"/> Examiner's Amendment/Comment                    |
| 4. <input type="checkbox"/> Examiner's Comment Regarding Requirement for Deposit<br>of Biological Material          | 8. <input checked="" type="checkbox"/> Examiner's Statement of Reasons for Allowance   |
|   | 9. <input type="checkbox"/> Other _____.   |

### **DETAILED ACTION**

1. Claims 1-5, 7-16, 18-26, 28, 29, 31-36, 38-46, 48-52, 54-56, and 59-66 were pending at the time of the previous Office Action. By the latest amendment, filed 4/17/06 claims 10, 19, 55, and 61 are cancelled. Therefore claims 1-5, 7-9, 11-16, 18, 20-24, 26, 28, 29, 31-36, 38-46, 48-52, 54, 56, 60, and 62-66 remain pending and have been examined.

### **EXAMINER'S AMENDMENT**

2. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it **MUST** be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with N. Rhys Merrett on 6-21-06.

Art Unit: 2137

IN THE SPECIFICATION:

Line 7 of page 1 of the Specification is amended to read as:

Reference is made to U.S. Patent Application No. 5,848,159, filed on December 8, 1998,

Art Unit: 2137

IN THE CLAIMS

Claim 26 lines 1 and 2 are amended to read as:

26. (currently amended) In a prime number generating system as recited in Claim ~~[[25]]~~ 26 further including the steps of:

Claim 1 line 10 is amended to read:

generated prime numbers whereby (k x t) tests are performed in parallel, each of the plurality

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

***Allowable Subject Matter***

3. Claims 1-5, 7-9, 11-16, 18, 20-24, 26, 28, 29, 31-36, 38-46, 48-52, 54, 56, 60, and 62-66 are allowed.

4. The following is an examiner's statement of reasons for allowance:

The closest prior art in the field, Menezes et al., "Handbook of Applied Cryptography," CRC Press 1996, Kent White, "Experiments in Parallel Processing for Undergraduate Students," 29th ASEE/IEEE Frontiers in Education Conference, and Daniel M. Gordon, "A Survey of Fast Exponentiation Methods", Journal of Algorithms 27, 1998, do not teach the combination of features of the applicant's invention as set forth in the independent claims, particularly including:

As per claims 1, 2, 15, 24, 28, 54, 64 and 65, performing a plurality of primality tests on a plurality of randomly generated prime numbers whereby the tests are performed in parallel, and where each of the plurality of primality tests include an associated exponentiation operation executed by an associated one of a plurality of exponentiation units.

As for claims 36 and 45, the arrangement of a plurality of exponentiation units, each communicatively coupled to a processor, where each includes a plurality of exponentiation units operating in parallel and responsive to one of a set of test parameters and operative to generate a primality test result for a prime number candidate declaring it composite or prime.

***Conclusion***

5. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paul E. Callahan whose telephone number is (571) 272-3869. The examiner can normally be reached on M-F from 9 to 5.

If attempts to reach the examiner by telephone are unsuccessful, the Examiner's supervisor, Emmanuel Moise, can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is: (571) 273-8300.

6-20-06

*Paul Callahan*

*Emmanuel L. Moise*  
**EMMANUEL L. MOISE**  
**SUPERVISORY PATENT EXAMINER**